CLAIMS

1. An integrated circuit comprising a processor and memory storing:

secret information accessible via a first address, the secret information comprising a string of bit values;

an inverse-string accessible via a second address, the inverse-string comprising a string of bit values, wherein each of the bit values in the inverse-string is the logical inverse of a bit value at a corresponding bit position in the secret information, the integrated circuit being programmed with code configured to:

(i) receive a request for the secret information; and

(ii) test whether the bit-values of the inverse string are the inverse of the bit-values at respective corresponding bit positions of the secret information.

2. An integrated circuit according to claim 1, configured and programmed to perform a defensive action in the event the test fails.

3. An integrated circuit according to claim 2, wherein the defensive action incudes deleting or destroying some or all of the contents of the memory in the event the test fails.

4. An integrated circuit according to claim 3, wherein the defensive action includes deleting or destroying the secret information and/or the inverse string.

5. An integrated circuit according to claim 3, wherein the defensive action includes preventing the processor from executing software.

6. An integrated circuit according to claim 3, wherein the defensive action includes resetting some or all of logic on the integrated circuit.

7. An integrated circuit according to claim 1, wherein the first and second addresses are at the same address in the memory.

8. An integrated circuit according to claim 7, wherein the string and inverse string are stored at different sub-addresses within the same address.

9. A method of ensuring validity of secret information stored in a memory in the form of a string of bit values accessible via a first address, the memory also storing an inverse-string accessible via a second address, the inverse-string comprising a string of bit values that are the logical inverses of the bit values at corresponding respective bit positions of the secret information, the method including the steps of:

receiving a request for the secret information; and

testing whether the bit-values of the inverse string are the inverse of the bit-values at respective corresponding bit positions of the secret information.

10. A method according to claim 9, further including the step of performing a defensive action in the event the test fails.

11. A method according to claim 10, wherein the defensive action incudes deleting or destroying some or all of the contents of the memory in the event the test fails.

12. A method according to claim 10, wherein the defensive action includes deleting or destroying the secret information and/or the inverse string.

13. A method according to claim 10, wherein the defensive action includes preventing execution of at least some code.

14. A method according to claim 10, performed by an integrated circuit, wherein the defensive action includes resetting some or all logic on the integrated circuit.

15. A method of manufacturing a plurality of the integrated circuits defined in claim 1, comprising the steps, for each of the plurality of integrated circuits, of:

storing the secret information and the inverse string at the first and second addresses in the memory of the integrated circuit; and

storing the code on the integrated circuit;

wherein the first and second addresses are randomly, pseudo-randomly or arbitrarily selected for each of the integrated circuits and the code for each integrated circuit is customised to know the first and second addresses of its secret information and inverse string.

16. A method according to claim 15, wherein the first and second addresses are restricted to one of two potential locations in the memory of each integrated circuit, the secret information and the inverse string for each integrated circuit being allocated to the first and second addresses randomly, pseudo-randomly or arbitrarily.

17. A method according to claim 15, wherein the secret information differs between at least two of the integrated circuits.